
# State of Maine
# Department of Administrative & Financial Services
# Office of Information Technology (OIT)

---

## Security Awareness Training Policy (AT-1)

---

## Table of Contents

## 1.0. Purpose

1.1. The purpose of this document is to outline the State of Maine's policy and procedures for security awareness and training. This corresponds to the Awareness and Training (AT) Control Family, of the National Institute of Standards and Technology (NIST) Special Publication 800-53 (Rev. 4).

## 2.0. Scope

2.1. This document applies to all State of Maine Executive Branch personnel, both employees and contractors.

## 3.0. Conflict

3.1. If this document conflicts with any law or union contract in effect, the terms of the existing law or contract prevail.

## 4.0. Roles and Responsibilities

4.1. *Agency Management:*

- 4.1.1. Enforces this policy as outlined in the compliance section (i.e., 7.0).
- 4.1.2. Establishes and conducts privacy training to meet regulatory requirements and business needs.
- 4.1.3. Ensures that agency personnel have access to, and receive, the *enterprise security awareness training*, at required intervals. This includes:
  - 4.1.1.1 Ensuring that agency personnel with access to state email receive the enterprise security awareness training delivered by the Office of Information Technology.
  - 4.1.1.2 Ensuring that agency personnel without access to state email are provided with alternative access to the enterprise security awareness training.
- 4.1.4. Determines agency personnel security awareness training requirements that extend beyond the enterprise security awareness training.
- 4.1.5. Ensures agency personnel are aware of all applicable penalties for non-compliance. (More in Section 7.0 of this policy).
- 4.1.6. Maintains agency personnel security awareness training records, in accordance with State of Maine, and any additional statutory records retention requirements.
- 4.1.7. Develops and implements agency-level policy and procedures, to meet any additional, federal statutory requirements pertinent to security awareness and training.

4.2. *OIT Information Security:*

- 4.2.1. Owns, executes, and shares responsibility for enforcement of this Policy.
- 4.2.2. Determines the training modules/content to be included in enterprise security awareness training.
- 4.2.3. Delivers enterprise security awareness training to agency personnel who have a state email account.

4.2.4. Makes training records available, for training delivered, to authorized agency personnel.
4.2.5. Consults with agencies to help determine the training delivery mechanisms/options to meet agency security awareness training requirements that extend beyond the enterprise security awareness training.
4.2.6. Conducts agency phishing exercises.

## 5.0. Management Commitment

5.1. The State of Maine is committed to following this document.

## 6.0. Coordination Among Agency Entities

6.1. The Office of Information Technology coordinates with agencies to deliver enterprise security awareness training in accordance with Executive Order 2014-003[1] .

## 7.0. Compliance

7.1. For State of Maine employees, failure to comply with this document may result in progressive discipline, up to and including dismissal.
7.2. For State of Maine contractors and non-State of Maine personnel, failure to comply may result in removal of the individual's ability to access, and use, State of Maine data and systems. Employers of contractors will be notified of any violations.
7.3. Personnel are also subject to any applicable penalties for statutory requirements compliance violations. Depending on the requirement, and the nature of the violation, penalties could include fines and/or criminal charges.
7.4. Two distinct compliance scenarios:
7.4.1. Failure to complete the mandated training within the mandated timeframe, and
7.4.2. Repeatedly failing the simulated phishing tests.
7.5. Failure to complete the mandated training within the mandated timeframe results in progressive discipline. This will be decided through collaboration between the Agency Management and the DAFS Bureau of Human Resources.
7.6. Repeatedly failing the simulated phishing tests results in a combination of additional, tiered Security training, and progressive discipline. The exact details of the additional, tiered Security training will be decided through collaboration between the Agency Management and the OIT Security Office. The OIT Security Office can provide the Agency Management with a suggested sample of additional, tiered Security training. But, ultimately, it is the Agency Management's responsibility to track and manage the details of the additional, tiered Security training. Any progressive discipline due to repeated failing of the simulated phishing tests will be decided through collaboration between the Agency Management and the DAFS Bureau of Human Resources.

[1] http://www.maine.gov/tools/whatsnew/attach.php?id=626944&an=1

## 8.0. Procedures

8.1. The following *standards* apply to the State of Maine's security awareness and training planning capabilities. They represent the base set of procedural requirements.

8.2. **Security Awareness Training (AT-2 including CE-2):**

8.2.1. Agencies must ensure their personnel receive enterprise security awareness training, which includes content on recognizing, and reporting, potential indicators of *insider threat*:

8.2.1.1. As part of initial training for new users (onboarding);

8.2.1.2. When required by information system changes; and

8.2.1.3. At least annually, thereafter.

8.2.2. State of Maine employee orientation informs new personnel of security awareness training requirements. New employees are informed about their duties regarding confidentiality, privacy, and conflict of interest, as documented in the Employee Handbook[2].

8.2.3. The Information Security Office delivers enterprise security awareness training, that includes content on recognizing and reporting potential indicators of *insider threat*, to agency users with email addresses by:

8.2.3.1. Querying Active Directory each month to identify new agency users. This is so agencies do not need to inform the Information Security Office of new hires.

8.2.3.2. Automatically pushing out enterprise security awareness training to new agency personnel (new Active Directory users).

8.2.3.3. Automatically pushing out enterprise security awareness training to agency personnel annually, thereafter.

8.2.3.4. Delivering enterprise security awareness training to agency personnel at other intervals, upon agency request (e.g., when required by information system changes).

8.2.3.5. Maintaining a list of agency personnel who have not received enterprise security awareness training.

8.2.3.6. Re-delivering training, at set intervals, as necessary.

8.2.4. Agencies are responsible for the delivery of enterprise security awareness training for any agency personnel without a State email address.

8.2.5. For each executive branch agency, the Information Security Office conducts quarterly phishing exercises that simulate actual cyberattacks. The schedule is randomized, so agency exercises could occur at any time during a particular quarter.

8.3. **Role-Based Security Training (AT-3):**

8.3.1. Agencies must determine the appropriate content of security training based upon the assigned roles and responsibilities of personnel, regulatory

[2] https://www.maine.gov/bhr/sites/maine.gov.bhr/files/inline-files/EmployeeHandbook.pdf

requirements, and the information systems to which personnel have authorized access.

8.3.2. Agencies must ensure that personnel with assigned security roles and responsibilities receive role-based security training:

8.3.2.1. Before authorizing access to information, an information system, or performing assigned duties that require access to *Personally Identifiable Information (PII)* or other *sensitive information;*

8.3.2.2. When required by information system changes; and

8.3.2.3. At least annually thereafter.

8.3.3. If agency security awareness training requirements extend beyond enterprise security awareness training, then the agency consults with the Information Security Office to help determine the training delivery mechanism/options.

8.3.4. The Information Security Office does not currently offer agencies role-based training, which is typically identified and fulfilled through individual professional development plans and/or through the training, testing, and exercise components of agency contingency or incident response plans.

8.3.5 OIT internally completes Role-Based security training as described in 8.3.4 and Contingency Plan Training, Testing and Exercise Procedures (IR-2, CP-3, IR-3, and CP-4).

8.4. **Security Training Records (AT-4):**

8.4.1. Agencies must retain individual training records in accordance with the State Archives Records General Retention Schedule[3], and any other applicable regulatory requirements for records retention.

8.4.2. The Information Security Office monitors and maintains security awareness training records for any training it delivers.

8.4.3. At the completion of training, personnel are instructed to keep their certificates of completion.

8.4.4. The training portal keeps a historical record of agency personnel who complete the training.

8.4.5. The Information Security Office makes agency training completion reports available to designated agency personnel, upon request.

## 9.0. Document Details

9.1. Initial Issue Date: 11 March 2014

9.2. Latest Revision Date: 22 June 2020

9.3. Point of Contact: Enterprise.Architect@Maine.Gov

9.4. Approved By: Chief Information Officer, OIT

9.5. Legal Citation: Title 5, Chapter 163: Office of Information Technology[4]

9.6. Waiver Process: Waiver Policy[5]

[3] https://www.maine.gov/sos/arc/records/state/generalschedules.html

[4] https://legislature.maine.gov/statutes/5/title5ch163sec0.html

[5] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/waiver.pdf

## 10.0. Review

10.1. This document will be reviewed annually, and when substantive changes are made to Policies, Procedures, or other authoritative regulations affecting this document.

## 11.0. Records Management

11.1. Office of Information Technology security policies, plans, and procedures fall under the *Routine Administrative Policies and Procedures and Internal Control Policies and Directives* records management categories. They will be retained for three (3) years, and then destroyed in accordance with guidance provided by Maine State Archives. Retention of these documents will be subject to any future State Archives General Schedule revisions that cover these categories.

## 12.0. Public Records Exceptions

12.1. Under the Maine Freedom of Access Act, certain public records exceptions may limit disclosure of agency records related to information technology infrastructure and systems, as well as security plans, procedures or risk assessments. Information contained in these records may be disclosed to the Legislature, or, in the case of a political or administrative subdivision, to municipal officials or board members under conditions that protect the information from further disclosure. Any aggrieved person seeking relief for an alleged violation of the FOAA may bring suit in any Superior Court in the state.

## 13.0. Definitions

13.1. *Enterprise Security Awareness Training:* The content includes a basic understanding of the need for information security and user actions to maintain security and privacy, and to respond to suspected security and privacy incidents. The content also addresses awareness of the need for operations security and privacy related to the organization's information security program.

13.2. *Insider Threat:* The potential for individuals (e.g., employees, contractors, former employees) to use insider knowledge of sensitive agency information (e.g., security practices, systems that hold sensitive data) to perform malicious actions, including unauthorized access or disclosure of Personally Identifiable Information (PII) or other sensitive information.

13.3. *Personally Identifiable Information (PII)*: Information which can be used to distinguish or trace the identity of an individual (e.g., name, social security number, biometric records, etc.) alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.). Source: NIST CSRC Glossary[6]. Maine state law has a more specific definition in 10 M.R.S. §1347[7].

[6] https://csrc.nist.gov/glossary

[7] http://legislature.maine.gov/legis/statutes/10/title10sec1347.html

13.4. *Sensitive Information*: Information that has the potential to cause great harm to an individual, government agency, or program if abused, misused, or breached. Sensitive information may include PII, and is protected against unwarranted disclosure, and typically carries specific criminal and civil penalties for an individual convicted of unauthorized access, disclosure, or misuse (e.g., Federal Tax, Protected Health, Criminal Justice, or Social Security information). Protection of sensitive information usually involves specific classification or legal precedents that provide special protection for legal and ethical reasons.

13.5. *Standard*: A collection of specific (technical and/or procedural) requirements that must be adhered to.